REMARKS

Claims 1-3 and 9-10 were rejected under 35 U.S.C. 103(a) over *Ashe* (U.S. Patent No. 6,014,745) in view of *Shimizu et al.*, ("*Shimizu*" U.S. Patent No. 6,085,323), in further view of *Kotani et al.* ("*Kotani*" U.S. Publication No. 2001/0008016). Applicant respectfully traverses this rejection in its entirety.

The present invention, as defined in the claims, is drawn to a data usage controlling apparatus that limits the usage of encrypted main data according to judgments made on encrypted condition information recorded on the same recording medium as the encrypted main data (Specification page 1 ll. 9-12). To establish the proper context for the independent claims, the data usage controlling system reads three items from a recording medium. These three items are:

main data that has been encrypted using a type 3 key (Unique key SK),

a type 2 key (Supplementary key R_A) that has been encrypted using a type 1 key (Random number R), and

encrypted condition information that has been encrypted using the type 2 key (Figure 8, and Specification page 13 ll. 6-10, page 19 ll. 9-21 and page 23 ll. 2-7).

The type 1 key is read from a predetermined storage unit 201 and is used to decrypt the supplementary key (Specification page 20 ll. 14-18 and page 23 ll. 7-10). The supplementary key is used to decrypt the usage conditions for the main data which may include an expiry date, a permitted number of executions, or a specified region of use, and includes a sequential encryption process using multiple keys (Specification page 15 ll. 13-17, page 20 ll. 2-3 and 18-21, and page 23 ll. 11-13).

If the decrypted usage conditions indicate main data usage is permitted, a unique key (type 3 key) is used to decrypt the digital contents M_A (Figure 10 and Specification page 20 ll. 24-27). Once the main data (digital contents) M_A is used, the data usage controlling system performs the following actions: updates the condition information I_A, updates the stored type 1 key, generates a new type 2 key, encrypts the updated condition information using the newly generated type 2 key, encrypts the newly generated type 2 key using the updated type 1 key, and replaces the encrypted type 2 key and the encrypted condition information with an encrypted newly generated type 2 key and an encrypted updated condition information on the recording medium (Figures 10-11, and Specification page 13 ll. 16-24 and page 22 line 20 to page 26 line 1). All of the remaining supplementary keys and condition information for the other digital contents on the recording medium are similarly decrypted, generated/updated, encrypted, and stored (overwritten) on the recording medium to replace the previous values whenever a single digital content is used (Figure 11 and Specification page 21 line 23 to page 22 line 11 and page 25 line 26 to page 26 line 1).

The process of <u>updating the supplementary keys and condition information</u> for each of the digital contents on the recording medium <u>is accomplished</u> for all digital contents <u>every time one</u> of the digital contents is used. In this manner, if the recording medium data were to be restored from a backup, for example, the digital contents would not be usable since the type 1 key is used to decrypt the type 2 key which is used for decrypting the condition information no longer matches the updated key. The type 1 key (Random number R) is updated after the use of any data contents, and hence would not match with the expected type 1 key of the restored recording medium, and subsequent access is prevented (Figure 14 and Specification page 25 ll. 17-24). In another aspect, if the update to the recording medium were somehow disrupted, the

type 1 key is still updated in the executing apparatus and the type 1 key would no longer match the expected type 1 key for subsequent accesses to the recording medium, and subsequent access is prevented (Specification page 26 ll. 4-12). Due to the update of the stored type 1 key in the executing apparatus, and the overwriting of the newly encrypted supplementary keys and condition information for each digital content in the recording medium, uncontrolled usage of the digital content is prevented and, in particular, the backup-restore attack for avoiding usage restrictions based on rewriting previous condition information is prevented.

The previously cited but not discussed reference to *Shimizu* is drawn to an information processing apparatus capable of storing data shared by a plurality of users and that is capable of protecting confidential information stored in the apparatus even if the apparatus is stolen and disassembled (Shimizu col. 2 ll. 28-40). This is accomplished by storing separately an external storage device carrying a set of master keys and a processing apparatus storing the encrypted data (Shimizu col. 7 ll. 31-49). *Shimizu* teaches that a master key is stored in a medium that is different from a recording medium in which a temporary key is stored, the master key can be added or deleted, and the master key is used for encrypting the temporary key and the encrypted temporary key is stored in the recording medium (*Shimizu* Figures 1 and 10, col. 6 line 62 to col. 7 line 30, and col. 13 ll. 43-46). However, Shimizu does not teach that the master key itself is updated in accordance with the usage of the main data in contrast with the present invention or even the master key is updated every time the main data is used, thus preventing a successful backup-restore attack since the updated key will not match a previously stored key.

The Office Action referred to the master key as corresponding to the type 1 key of the present invention and the temporary key as corresponding to the type 2 key of the present invention. Applicant respectfully submits that the temporary key disclosed by *Shimizu* is

different from the type 2 key of the presently claimed invention for two reasons. First, the temporary key is not used for decryption before the main data is used. Second, the temporary key is not updated after the main data is used (*Shimizu* Figures 8-10 and col. 12 ll. 33-62).

The *Shimizu* reference is cited in the Office Action as disclosing an updating means and method for updating the type 1 key stating a plurality of master keys exist, each of which may be updated upon authentication of a password (*Shimizu* col. 13 ll. 14-53). *Shimizu* teaches the designation of a particular master key based on certain user information, but does not teach updating the condition information nor selectively accessing encrypted data based on the condition. Applicant respectfully traverses the assertion that *Shimizu* teaches the updating means and method for updating the type 1 key as presently claimed because *Shimizu* does not teach a first updating means for updating the condition information in accordance with usage of the main data.

The newly cited *Kotani* reference is drawn to an information management method for restoring lost electronic data from a backup copy of the data and generating a corresponding encrypted portion of the lost data from other portions of the restored data (*Kotani* page 1 para. [0012]-[0015], page 4 para. [0074], and page 5 para. [0085]). In this way, lost licensing information that was encrypted and stored in a certain area of a recording medium, such as a particular optical layer of a re-writeable disc, can be determined from other portions of the recording medium data and restored (*Kotani* page 3 para. [0055] and page 6 para. [0102]).

The *Kotani* reference is cited in the Office Action as disclosing an updating means and method for updating the condition information (*Kotani* page 5, para [0080]-[0081]). Applicant respectfully traverses the assertion that *Kotani* teaches the updating means and method for updating the condition information as presently claimed since *Kotani* is using the term update to

mean restoring the original licensing data, not generating different condition information or different encryption keys (*Kotani* page 5 para. [0085]). The *Kotani* reference teaches encrypted license information is read out from a third layer, decrypted, and recorded in a second layer (*Kotani* 7 and page 4 para. [0074] to page 5 para. [0076]). Applicant respectfully submits that this does not mean that original license information is replaced with new license information when the encrypted license information is recorded in the second layer. *Kotani* clearly teaches that <u>lost information can be restored</u> from a backup copy and <u>then utilized as before the loss occurred</u> (Kotani page 2 para. [0023]).

Applicant respectfully submits this is actually distinctly different from the objects and effects of the present invention where prior data cannot be restored from a backup and successfully utilized. The type of operation taught by *Kotani* is distinct from the presently claimed invention in which the condition information stored in the recording medium is replaced with different updated condition information that has been newly encrypted.

As previously discussed, the *Ashe* reference is drawn to a method of accessing proprietary information stored in a remote memory device such as an Electrically Erasable Programmable Read Only Memory (EEPROM) (Ashe col. 1 ll. 36-39). *Ashe* is addressing the problem of interception of the proprietary data as it is read from the EEPROM, where the proprietary information stored in the remote memory device could be viewed by a hostile third-party if the proprietary information is not protected through encryption. *Ashe* teaches that a processor reads an encrypted key Zi from a portion of the memory, decrypts Zi into Kc using a master key and a first algorithm (*Ashe* col. 1 ll. 45-47 and col. 2 line 66 to col. 3 line 1). Once Kc is determined, the proprietary information is decrypted using a second algorithm and may be utilized by the processor in an unlimited manner (*Ashe* col. 3 ll. 1-6). The master key and first

algorithm is shared among all of the processors, so the master key cannot be changed through an update, for example, or else the system taught by Ashe would fail. Further, *Ashe* does not disclose any of the operations described above in accordance with the usage of main data governed by condition information, such as a permitted number of uses, for example. *Ashe* teaches a system where, once the master key is compromised, unlimited and uncontrolled access is granted to the proprietary information, assuming the decryption algorithms are known. The Office Action suggests that although *Ashe* does not disclose and updating means for the condition information and the type 1 key, the generating means for generating a new type 2 key, nor replacing an encrypted key (understood to be only Zi), as an alternative the algorithm unique to the program being encrypted may be encrypted as well. Applicant respectfully submits that the encryption of the second algorithm Ec taught by *Ashe* is not relevant, and is suggested as an alternative by *Ashe* in order to safeguard the algorithm and avoid having to store the algorithm in the clear either within the memory. *Ashe* does not teach changing the algorithm, or updating anything. In fact, *Ashe* does not teach that the memory itself is writeable by the processor, and it is commonly understood that the "Read Only Memory" EEPROM, prohibits selectively updating of the memory by the processor except perhaps in a non-operational or initialization sense where the EEPROM is taken out of ordinary service and reprogrammed.

Regarding independent Claim 1, the structure of the

> "first updating means for updating the condition information in accordance with usage of the read main data"; and the
>
> "second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data"

is neither taught nor suggested by any of the references in any combination, as described above. Applicant respectfully submits that the cited references, even if combined as suggested, do not teach all of the claimed elements, as described in reference to each of the cited references above. Independent Claim 9 is a data usage controlling method in accordance with Claim 1 and is believed allowable over the cited references for the reasons stated regarding independent Claim 1. Similarly, independent Claim 10 is a computer-readable recording medium storing a program in accordance with Claim 1 and is also believed allowable over the cited references for the reasons stated regarding independent Claim 1.

Regarding independent Claim 2, in addition to the arguments associated with the cited references and the arguments regarding Claim 1, the structure of the

> "generating means for generating a new type 2 key in accordance with usage of the main data";
>
> "updating means for updating the type 1 key in the storage unit after the decrypting means has decrypted all (n-1) encrypted type 2 keys"; and the
>
> "second encrypting means for encrypting the (n-1) type 2 keys and the new type 2 key using the updated type 1 key and replacing all n encrypted type 2 keys on the recording medium with the newly encrypted type 2 keys"

is neither taught nor implied by the references in any combination. None of the references teach the operating of generating and updating keys based on the usage of a main data as claimed. So, by extension, these references cannot teach an updating process for a plurality of keys as claimed.

Claims 3-8 depend from independent Claim 2 and are believed allowable based on the above arguments regarding the cited references and Claim 2.

Applicant respectfully requests this rejection be withdrawn.

Claims 5-6 were rejected under 35 U.S.C. 103(a) over *Ashe* and *Shimizu* and *Kotani* in view of *Inazawa et al.* ("*Inazawa*" U.S. Patent No. 6,587,948). Applicant respectfully traverses this rejection in its entirety.

Contrary to the present invention, the previously discussed *Inazawa* reference is drawn to a recording method and apparatus in which digital data is recorded onto a disc as run-length limited code by modulating digital data used for modulating marks or spaces on the disc and, at the same time, the recorded digital data is encrypted by using key data which is also recorded onto the same disc by variation of the shape of marks or spaces with timing having no effect on the leading and trailing edges of the marks and spaces (*Inazawa* col. 1 ll. 8-15). *Inazawa* teaches a recording and playback method where encrypted data is recorded onto an optical disc using a technique that superimposes a decryption key on the optical encoded elements themselves in a dimension orthogonal (transverse) to the direction of reading the encrypted data itself (Figures 19A-19D). Even though it is well known to use encryption in general to protect data from illegal copying, *Inazawa* does not teach the novel usage control techniques to provide controlled access to encrypted content of the present invention including replacing the encrypted condition information on the recording medium with newly encrypted condition information, as claimed. *Inazawa* describes the types of copying addressed by his solution as relating to illegal copies produced by using a result of decoding a master key, and illegal copies produced by physically copying a pit form (optical pattern) from a legally created optical disc (*Inazawa* col. 2 ll. 36-50).

Inazawa is cited in the Office Action as disclosing the main data in each set on a recording medium being encrypted using a type 3 encryption key identified as a disc key DK

(*Inazawa* col. 6 ll. 57-63). Further, *Inazawa* is cited as disclosing an obtaining means for obtaining the type 3 key (disc key DK) and a second decrypting means for decrypting the read main data using the obtained type 3 encryption key (*Inazawa* col. 6 ll. 57-63). Applicant respectfully traverses the assertion that *Inazawa* teaches the obtaining means for obtaining the type 3 key and a second decrypting means for decrypting the read main data using the obtained type 3 encryption key as presently claimed because the disk key DK taught by *Inazawa* is not a type 3 decryption key used within the context of a previously described type 1 key and a type 2 key in the independent Claim 2. The disk key DK is merely an initial configuration string for a plurality of scramblers/descramblers to modulate/demodulate a stream of data using pseudo-random exclusive OR circuit structures which allow the data to be obtained one bit at a time (*Inazawa* Figures 4 and 6, col. 6 ll. 8-9, and col. 7 line 46 to col. 8 line 9). To properly select/extract the desired stream of data, additional information in the form of scrambler-identification data SID is used to select one stream of data from the plurality of streams (*Inazawa* Figure 4 and col. 6 ll. 21-24).

Inazawa teaches the use of a master key KM that is similarly used to decode/demodulate the data encoded on the optical disc (*Inazawa* col. 5 ll. 51-63). However, it is important to observe that neither the disc key DK, nor the master key KM are changed, updated, or written back to the recording medium. Further, once the optical disc with the special transversal encoding of data is completed, it is clear the usage of the optical disc based medium is a read-only operation, and no data is written back to the optical medium. Applicant respectfully suggests this read-only approach teaches away from both the newly cited *Kotani* reference as well as the context of the independent Claim 2 from which Claims 5 and 6 depend, where both the first and the second keys are changed. Further, there is no teaching in any of the references

other than *Inazawa* that would lead a person of ordinary skill in the relevant art to combine the cited references in the stated manner since *Inazawa* teaches a read-only medium while *Ktoani* requires a writeable medium. The Office Action suggests the disc key DK can be used to prevent illegal copies. Applicant respectfully submits that *Inazawa*. teaches it is the technique of recording the key data by a physical modulation of the optical pit shape in the width direction that makes it difficult to produce usable, illegal copies, and not the disc key DK itself (*Inazawa* Figures 19A-19D and col. 20 ll. 16-24).

Inazawa is not focused on simple encryption, complex sequential encryption with multiple keys, nor on encryption only as a protection against copying, but instead teaches a particular kind of optical encoding that foils physically copying an optical disc and reproducing usable data. Applicant respectfully submits that there cannot be any teaching in *Inazawa* towards the use of the particular type of content encryption encoding that encompasses a <u>condition information that is updated and stored</u> on the optical medium since any alteration of the content data of the optical disc, assuming it can be altered at all, would necessarily change the pit form pattern, and the encryption information would be lost. Applicant respectfully submits, therefore, that even if it is possible to combine the teachings of *Inazawa* with the other cited references, the combination does not teach the presently claimed invention. Applicant respectfully submits that because of the differences discussed above, that there is no motivation to combine these references, and even if they are combined as suggested, they do not teach the presently claimed invention. Further, Claims 3-8 depend from independent Claim 2 and are believed allowable based on the above arguments regarding the cited references and Claim 2, as discussed above.

Applicant respectfully requests this rejection be withdrawn.

Claims 4, and 7-8 were rejected under 35 U.S.C. 103(a) over *Ashe* and *Shimizu* and *Kotani* in view of *Marino et al.* ("*Marino*" U.S. Patent No. 6,026,165). Applicant respectfully traverses this rejection in its entirety.

Contrary to the present invention, the previously discussed *Marino* reference is drawn to a secure wireless communications system that uses a variable key for encryption and decryption, where the key may be updated based user input along with a sequence number (*Marino* col. 1 ll. 5-12 and col. 3 ll. 30-35). The sequence number is used to synchronously order the message sequence at both the transmitter and the receiver, and the user may update and re-register a new random number at any time (*Marino* col. 3 ll. 35-42). *Marino* teaches a "de-registering" of at least one and possibly all transmitters at the same time (*Marino* col. 3 ll. 45-48 and col. 4 ll. 31-59). To register any of the transmitters with the receiver, a new random number is generated by the transmitter and sent along with a transmitter identification code to the receiver as a part of an initialization process (*Marino* col. 3 ll. 54-63). The new random number key is used along with a sequence number to encrypt subsequent messages from the newly registered transmitter to the receiver (*Marino* col. 3 line 63 to col. 4 line 3). This new random number key and initial sequence number may be encrypted prior to sending, but the encryption and decryption is accomplished using algorithms and keys that are common to (assumed held within) each of the receivers and transmitters (*Marino* col. 4 ll. 3-5). Hence, *Marino* teaches encryption of messages using a variable key, but that random number key is updated by a user action and is not related to permitted usage of the data itself. Even if it is assumed that the sequence number is analogous to "condition information", the sequence number is used as part of the encryption key and not as encrypted information that governs access to other encrypted information (*Marino* col. 3 ll. 32-35). *Marino* does not teach the use or encryption of condition information in accordance with

the usage of the read main data, as claimed, which is hypothetically assumed for the sake of analysis to be the transmitted or command data. As a result, *Marino* cannot teach an updating means for the condition information. Even if it is assumed for the sake of argument that *Marino* teaches a type 1 key that is updated, *Marino* cannot teach a generating means for generating a new type 2 key as claimed since the only other encryption taught by *Marino* is a static encryption of the initial registration message itself using a common key that is not updated. Hence, *Marino* does not teach either the objects or the effects of the present invention.

The *Marino* reference is cited in the Office Action as disclosing a generating means in the form of a sequence number generator that generates a new type 2 key every time a user makes a predetermined number of uses of the main data on the recording medium (*Marino* col. 7 ll. 14-46). Applicant respectfully traverses the assertion that *Marino* teaches the generating means as presently claimed because none of the references teach updating keys based on the usage of main data, as previously discussed regarding Claims 1 and 2. In context, the cited portion of the Marino reference is drawn to the creation of a data message that includes both fixed and variable data represented in both encrypted and unencrypted data fields, but encryption key itself is <u>not</u> actually sent during normal operations (*Marino* col. 7 ll. 14-46). *Marino* teaches that a random number is generated by the random key generator 21 and stored in both the transmitter and the receiver during a "(learning)" or initialization process where the random number is sent to the receiver for use as a encryption key and that this initialization process is not part of the normal operation of his described invention (*Marino* Fig. 2 and col. 20-29). The Device ID identification number from the transmitter is used to "look up" the stored encryption key in the receiver while the sequence number is used to validate the order of commands

received by comparison with the previous sequence number received from the transmitter (*Marino* col. 7 ll. 32-35).

Regarding Claim 4, Applicant respectfully submits that the structure of a

> "generating means [that] generates a new type 2 key every time a user makes a predetermined number of uses of the main data"

is neither taught nor suggested by any of the references.

Similarly, regarding Claims 7 and 8, *Marino* cannot teach updating a type 1 key as claimed since the encryption key for Marino is set once during the learning or initialization process and then used by the receiver after a successful lookup based on the Device ID from the transmitter (*Marino* Fig. 2 and col. 20-29). Since *Marino* does not teach updating type 1 keys as claimed in the present invention, Applicant respectfully submits that it is irrelevant what calculations *Marino* teaches including adding one to a previous sequence number.

Finally, Claims 3-8 depend from independent Claim 2 and are believed allowable based on the above arguments regarding the cited references and Claim 2.

Applicant respectfully requests this rejection be withdrawn.

It is believed that all claims are in condition for allowance, and an early notification of the same is requested.

If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this document and appropriate fee are being deposited with the U.S. Postal Service as first class mail under 37 C.F.R. § 1.8 and is addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 1, 2004.

By: Joan M. Gordon

Joan M. Gordon
Signature

Respectfully submitted,

SNELL & WILMER L.L.P.

Ketan S. Vakil

Ketan S. Vakil
Registration No. 43,215
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4905